Deployable DNS

Why Should You Care?

Ray Buschur

30 August 2001

Organization: W114
Project: 0701A340-AT

MITRE

Business Drivers

- Army is revising its approach to provisioning IT services
  - Increased awareness of the cost of provisioning IT
  - Budgets are not expanding as quickly as demands
  - Army Knowledge Management will address some of these issues
- Logistical systems are becoming more sophisticated
  - Just in time logistics transition
  - DRID 54 - Directing web based logistics
    - Discussions are on going about where the servers will reside in the architecture
  - Public Key Infrastructure (PKI) enabled applications
- Network Operating Systems are becoming more capable
  - Tracking network inventory
  - Allocation and authorization of roles based on policy
  - Security has been increased and enhanced

PKI Enabled Infrastructure

- DoD has directed that all network infrastructure be PKI enabled by Oct ‘02
  - What does that mean?
    - Web servers pass users certificates to verify they are the web server the user intended to access
    - Mail servers will not accept connections from client systems that it can not verify using X.509 certificates
- X.509 Device certificates include the fully qualified domain name of the network element, as a part of the certificate
  - A certificate is invalidated when a host changes any part of its fully qualified domain name (FQDN)
    - Example: buschurPC.mitre.org - FQDN
      buschurPC - host name or owner
      mitre.org - domain name

Microsoft Windows 2000 & Active Directory

- W2K security architecture allows membership in only one domain at a time
  - Switching can take a great deal of time and may cause problems
  - Resource sharing can still be accomplished but involves a more user intervention
- Active Directory tracks computers by their fully qualified domain name (FQDN) my-pc.1stbde.4id.army.mil
  - AD uses FQDN to identify hosts within the directory
  - AD requires hosts have a static FQDN
  - Changing a system's FQDN could result in users not being able to access to their STAMIS applications or other network resources such as printers

Intra-enclave Requirements

- Windows 2000 clients moving within the enclave should be provided ubiquitous network service
  - The client's FQDN should not change as it moves between separate LAN segments
    - This enables the Windows 2000 Active directory to recognize the client when physically located at different points on the network
- Device certificates should not require maintenance when hosts are relocated within the enclave
  - At a minimum the FQDN must remain stable even though the network element is physically relocating on the network and using different IP address space

Open Discussion